

كيف يستخدم «الهاكرز» الذكاء الاصطناعي؟

ميديا وتلفزيون | تكنولوجيا | الأخبار | الثلاثاء 28 أيار 2024 | 13:50

يوفّر الذكاء الاصطناعي أدوات جديدة بالغة القوة لعصابات القرصنة السيبرانية، تمكّنها من العمل على المستوى الدولي أكثر من أي وقت مضى، وفقاً لتقرير علمي نشرته مجلة MIT Technology Review في 21 أيار (مايو) الحالي.يتيح الـ AI أتمتة المهام وإنتاجها بسرعة مثل إنشاء رسائل بريد إلكتروني للتصيّد الاحتيالي، وإنشاء صور مزيّفة عميقة، واستخراج البيانات الشخصية التي قد تتطلب عملاً مضنياً. لكن تطوّر أنظمة الـ AI مثل نماذج اللغة الكبيرة (تشات جي بي تي وغيره) مكّن المجرمين من إنشاء محتوى مُقنع وفيديو حقيقياً لا يمكن كشفه بسهولة.

فيما يلي 5 أساليب يستخدمها «الهاكرز» للقرصنة عبر الذكاء الاصطناعي:

1. التصيّد (Phishing)

أكبر حالة استخدام للذكاء الاصطناعي التوليدي بين «الهاكرز» في الوقت الحالي هي التصيّد الاحتيالي، وتتضمن محاولة خداع المستخدمين للكشف عن معلومات حسّاسة يمكن استخدامها لأغراض ضارة. وحذر باحثون أمنيون من بينهم الباحث في مجال أمن الذكاء الاصطناعي في ETH Zurich، ميسلاف بالونوفيتش، من أن مجرمي الإنترنت يستغلون الارتفاع السريع لأنظمة مثل ChatGPT لتعزيز هجمات التصيّد الاحتيالي عبر الإنترنت. ويستفيد المجرمون من الخدمات التي تدمج القدرات اللغوية لـ ChatGPT لترجمة الرسائل إلى الضحايا عبر اللغات وإعادة كتابتها لتبدو حقيقية أكثر. وقال الباحث في مجال التهديدات لدى «تريند مايكرو»، فينسينزو سيانكاجليني، إنّه «في السابق، كان من السهل نسبياً اكتشاف ما يسمى بحيلة «الأمير النيجيري» (عندما تَعِد رسالة إيميل، الضحية، بمبلغ كبير من المال مقابل دفعة صغيرة مقدماً) لأن اللغة الإنكليزية المستخدمة كانت ضعيفة، لكن تسمح نماذج اللغة الآن للمحتالين بإنشاء رسائل تبدو وكأن متحدثاً أصلياً في اللغة كتبها». كما تساعد نماذج الـ AI المُحسّنة المتعدّدة اللغات الجماعات الإجرامية على التنسيق دولياً وتنفيذ عمليات احتيال معقّدة وواسعة النطاق عبر الحدود.

2. عمليات الاحتيال الصوتي العميقة

سمح الذكاء الاصطناعي التوليدي بتطوير التزييف العميق بشكل كبير، فأصبحت الصور ومقاطع الصوت والفيديو الاصطناعية تبدو أكثر واقعية. وفي وقت سابق من هذا العام، تعرّض موظف في هونغ كونغ للاحتيال بمبلغ 25 مليون دولار، بعدما استخدم مجرمو الإنترنت تزييفاً عميقاً لمدير الشركة المالي لإقناع الموظّف بتحويل الأموال إلى حساب الهاكر.

3. تجاوز عمليات التحقق من الهوية

يستخدم القراصنة التزييف العميق بطريقة أخرى أيضاً عبر تجاوز أنظمة التحقّق «اعرف عميلك». وتستخدم البنوك وبورصات العملات المشفّرة هذه الأنظمة للتحقّق من أنّ عملاءها هم أشخاص حقيقيون. وتقدّم مجموعات قرصنة خدمة تزييف بطاقة هوية عبر وضع صورة الشخص المُراد انتحال صفته فوق وجه الشخص الحقيقي على البطاقة، لخداع نظام التحقّق عبر كاميرا الهواتف الذكية العاملة بنظام التشغيل «أندرويد»، من أجل دخول حسابه على موقع Binance للعملات المشفّرة. ووجد تقرير المجلة أن بعض الجهات الإجرامية تقدم تلك الخدمة مقابل مبلغ زهيد يصل إلى 70 دولاراً أميركياً.

4. تحرير الذكاء الاصطناعي من قيوده

تهدف شركات الذكاء الاصطناعي إلى تقييد الاستخدام غير القانوني لتقنياتها. فإذا سُئلت أنظمة الـ AI عن كيفية صنع قنبلة، لن تُقدم إجابة مفيدة. وهذه القيود على المعرفة في هذا الجانب ضرورية جداً. لكن بدأ القراصنة في تبنّي اتجاه كسر الحماية والقيود على الـAI بغية استخراج معرفة تشكل خطراً على الناس.

5. جمع المعلومات والمراقبة

يقول بالونوفيتش إنّ نماذج اللغة الكبيرة تُعدّ أداة مثالية، ليس فقط للتصيّد الاحتيالي، ولكن أيضاً لجمع المعلومات الشخصية (الكشف عن معلومات خاصة وتحديد هوية شخص ما عبر الإنترنت). فقد دُرّبت على كميات هائلة من بيانات الإنترنت، بما في ذلك البيانات الشخصية، ويمكنها استنتاج المكان الذي يمكن أن يتواجد فيه شخص ما.

ينقل تقرير مجلة MIT Technology Review تحذير خبراء الأمن من أنّ زيادة التنسيق بين الجماعات الإجرامية في جميع أنحاء العالم يمثل خطراً كبيراً مع تحسن نماذج الـ AI مثل «تشات جي بي تي». ويحثّون الشركات على الاستثمار في حماية البيانات والأفراد على توخّي الحذر بشأن المعلومات الشخصية التي يشاركونها عبر الإنترنت والتي يمكن استغلالها بواسطة أنظمة الذكاء الاصطناعي.